Facultad de Ciencias Sociales y de la Comunicación

Grado en Gestión y Administración Pública

Asignatura de:

Redes de datos

Tema III:

Protocolo TCP/IP

(Transparencias de clase)

DEPARTAMENTO DE INGENIERÍA INFORMÁTICA

Profesor: Manuel Fernández Barcell

e-mail: manuel.barcell@uca.es
www.mfbarcell.es

Indice

El objetivo de este tema es presentar algunos conceptos básicos en relación con el protocolo TCP/IP , las direcciones IP, los dominios, las formas de traducción de nombres

1.1 La familia de protocolos INTERNET

Internet es una red formada por un conglomerado muy amplio y extenso de equipos en el que se se encuentran ordenadores con sistemas operativos distintos, distintos tamaños y distintos servicios. Ante tanta diversidad resulta necesario establecer un conjunto de reglas comunes para la comunicación entre estos diferentes elementos y que además optimice la utilización de recursos tan distantes. Este papel lo tiene el protocolo TCP/IP.

La red **Internet** es una Red global de ordenadores (una red de redes) cuya característica común es que usan para comunicarse el protocolo **TCP/IP**.

1.2 Protocolo TCP/IP (*Transmission Control Protocol/Internet Protocol*)

Más que un protocolo, **TCP/IP** es un conjunto de protocolos de red, capaces de soportar las comunicaciones entre equipos conectados a gran número de redes heterogéneas, independientes de un vendedor.

Su origen es: solucionar las comunicaciones a través de la red **ARPANET** para **DoD** Departamento de Defensa de USA (*Departamen of Defense 1.972*).

Comienza su utilización en DARPA (Agencia de proyectos de investigación avanzada para la defensa).

En 1983 se convierte en estándar para **DoD** (ARPANET + MILNET) (*Defense Data Network* DDN).

Te recomiendo que busques el la www.wikipedia.org el concepto internet. Encontraras información muy interesante.

En http://www.aui.es/historia/ihistoria.htm puedes encontrar una historia de Internet.

CARACTERÍSTICAS DE TCP/IP

Las principales características son:

- Utiliza conmutación de paquetes.
- Proporciona una conexión fiable entre dos máquinas en cualquier punto de la red.
- Ofrece la posibilidad de interconectar redes de diferentes arquitecturas y con diferentes sistemas operativos.
- Se apoya en los protocolos de más bajo nivel para acceder a la red física (*Ethernet, Token-Rin*g).

FUNCIONAMIENTO DE TCP/IP

Una red TCP/IP transfiere datos mediante el ensamblaje de bloques de datos en paquetes conteniendo

- La información a transmitir.
- La dirección IP del destinatario.
- La dirección IP del remitente.
- Otros datos de control.

Los dos protocolod básicos de **TCP/IP** son TCP e IP para el transporte y transmisión de datos respectivamente.

- **TCP:** Coordina el movimiento de datos entre ordenadores dividiendo dichos datos en paquetes.
- **IP**: Mueve los datos de un ordenador a otro.
  Los paquetes pueden ir por caminos distintos.
  El receptor los reordena.
  Si un paquete llega mal, se retransmite sólo ese paquete.

TCP/IP entrega datos en forma estándar y hace que estén disponibles para ser utilizados por programas de más alto nivel.

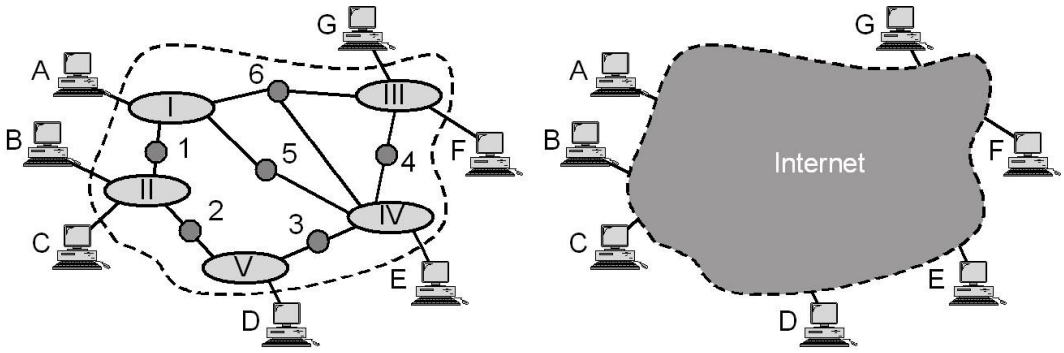
1.2.1 Los protocolos

Hay dos tipos de comunicaciones:

- **Orientada a la conexión**. Usa *circuitos virtuales* para la transmisión. Un circuito virtual proporciona una aparente línea directa de comunicación entre dos procesos. Los servicios orientados a la conexión incorporan secuenciamiento automático, control de errores y control de flujo.
- **Sin conexión.** Usa *datagramas* para la transmisión. Cada *datagrama* es un mensaje independiente. Son servicios orientados a la transacción (*transaction-oriented*), y no ofrecen normalmente garantías sobre los retrasos y duplicaciones.

Para estas distintas formas de comunicación se utilizaran protocolos distintos.

El protocolo de comunicaciones denominado **TCP/IP** se encuentra constituido en realidad por dos protocolos: el **TCP** y el **IP**.



a. Una internet real b. Una internet vista por TCP/IP

Protocolo TCP

El protocolo **TCP** (Protocolo de Control de Transmisión) es el encargado de tomar la información que se desea transmitir y dividirla en paquetes o segmentos. Además enumerará cada paquete para que el receptor pueda verificar la información y ponerla en el orden adecuado. En el destinatario, una parte del software de TCP, extrae la información de dichos paquetes y los ordena adecuadamente. Si algún paquete se pierde durante la transmisión, el receptor solicita su retransmisión al emisor. Una vez que el protocolo TCP tiene toda la información en el orden adecuado, la pasará a la aplicación o programa que esté utilizando sus servicios.

Otros protocolos de transmisión: UDP

Establecer una conexión TCP exige una gran cantidad de trabajo y de tiempo. De forma que si la información a enviar es poca (del orden de un paquete) y no es necesario garantizar su entrega, las características del protocolo TCP pueden estar desaprovechadas.

Para estos casos existe otro protocolo estándar denominado **Protocolo de Datagramas de Usuario** o **UDP**. Este es utilizado en algunas aplicaciones en lugar del protocolo TCP. El protocolo UDP es mucho más sencillo, porque no se preocupa de que los paquetes de información se pierdan, ni de que lleguen en un orden determinado. El UDP se utiliza comúnmente en programas que envían mensajes cortos y que sólo se reenvían si no reciben respuesta en un tiempo determinado.

Protocolo internet (IP)

El protocolo IP es el encargado de etiquetar cada paquete de información con la dirección de la máquina origen y de destino apropiadas. Cada ordenador conectado a Internet tiene una dirección Internet (IP *address*) que es única y exclusiva y que lo distingue de cualquier otro ordenador perteneciente a Internet.

Todo programa o aplicación de Internet necesita conocer el número IP del ordenador con el que quiere comunicarse. Sin embargo, como ya se verá más adelante, el usuario no necesita saber esa información, ya que existe un sistema de nombres más sencillo para referirse a una dirección.

El protocolo IP se encarga, por tanto de tomar los paquetes TCP, que contenían los segmentos de información, así como información adicional para reordenar y detectar errores en el destino, y les añade las direcciones IP de las máquinas origen y destino, generando un nuevo paquete IP que ya puede ser transmitido por la red.

Se trata de un protocolo a nivel de red cuyas principales características son:

- Ofrece un servicio no orientado a la conexión; esto significa que cada trama en la que ha sido dividido un paquete es tratado por independiente. Las tramas que componen un paquete pueden ser enviadas por caminos distintos e incluso llegar desordenadas.
- Ofrece un servicio no muy fiable porque a veces los paquetes se pierden, duplican o estropean y este nivel no informa de ello pues no es consciente del problema.

1.3 Arquitectura Internet

1.3.1 Capas

En la siguiente figura vemos la relación entre los niveles de **internet** y los del modelo de referencia de la ISO/OSI.

<table>
<tr><th colspan="2">Niveles Internet</th><th>Niveles ISO</th></tr>
<tr><td colspan="2" rowspan="3">Aplicaciones</td><td>Aplicación</td></tr>
<tr><td>Presentación</td></tr>
<tr><td>Sesión</td></tr>
<tr><td>Transmision Control Protocol
(TCP)</td><td>User Datagram Protocol
(UPD)</td><td>Transporte</td></tr>
<tr><td colspan="2">INTERNET PROTOCOL
(IP)</td><td rowspan="2">Red</td></tr>
<tr><td colspan="2">INTERFACES</td></tr>
<tr><td colspan="2" rowspan="2">MEDIO FISICO</td><td>Enlace de datos</td></tr>
<tr><td>Físico</td></tr>
</table>

En el modelo TCP/IP se pueden distinguir cuatro capas:

- La capa *host*-red
- La capa internet
- La capa de transporte
- La capa de aplicación

Pasemos a describirlas brevemente.

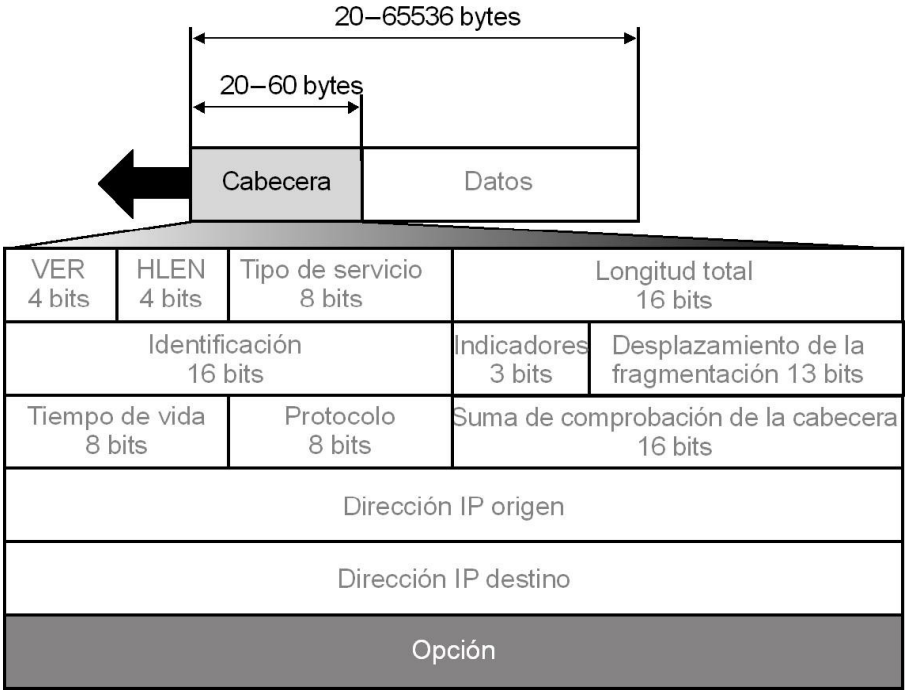
La capa *host*-red

Esta capa engloba realmente las funciones de la capa física y la capa de enlace del modelo OSI. El modelo TCP/IP no dice gran cosa respecto a ella, salvo que debe ser capaz de conectar el *host* a la red por medio de algún protocolo que permita enviar paquetes IP. Podríamos decir que para el modelo TCP/IP esta capa se comporta como una 'caja negra'. Cuando surge una nueva tecnología de red (por ejemplo ATM) una de las primeras cosas que aparece es un estándar que especifica de que forma se pueden enviar sobre ella paquetes IP; a partir de ahí la capa internet ya puede utilizar esa tecnología de manera transparente.

La capa internet

Esta capa es el 'corazón' de la red. Su papel equivale al desempeñado por la capa de red en el modelo OSI, es decir, se ocupa de encaminar los paquetes de la forma mas conveniente para que lleguen a su destino, y de evitar que se produzcan situaciones de congestión en los nodos intermedios. Debido a los requisitos de robustez impuestos en el diseño, la capa internet da únicamente un servicio de conmutación de paquetes no orientado a conexión. Los paquetes

pueden llegar desordenados a su destino, en cuyo caso es responsabilidad de las capas superiores en el nodo receptor la reordenación para que sean presentados al usuario de forma adecuada.

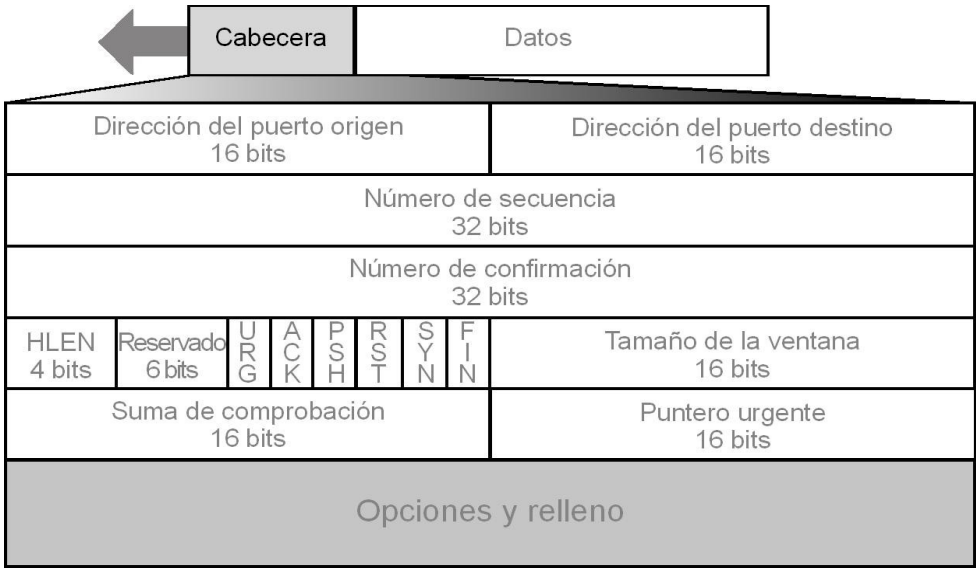


paquete IP

A diferencia de lo que ocurre en el modelo OSI, donde los protocolos para nada intervienen en la descripción del modelo, la capa internet define aquí un formato de paquete y un protocolo, llamado IP (*Internet Protocol*), que se considera el protocolo 'oficial' de la arquitectura.

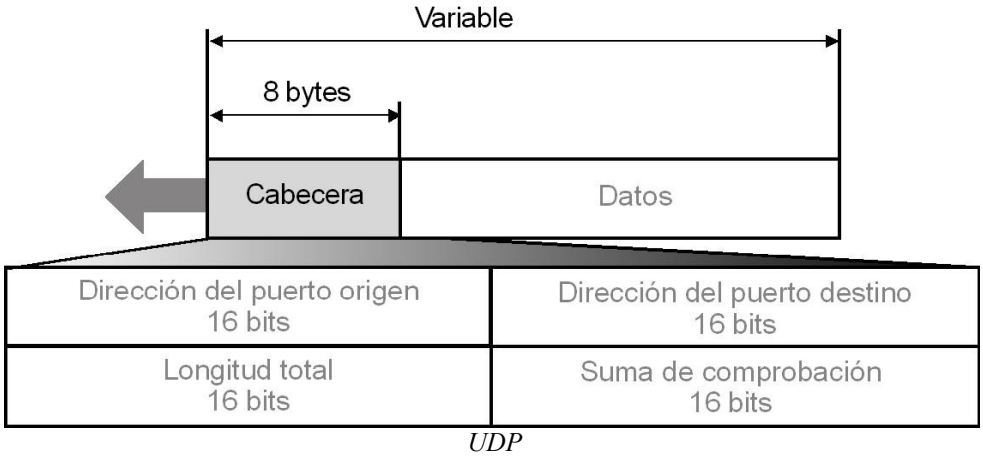
La capa de transporte

Esta capa recibe el mismo nombre y desarrolla la misma función que la cuarta capa del modelo OSI, consistente en permitir la comunicación extremo a extremo (*host* a *host*) en la red. Aquí se definen dos protocolos: el TCP (*Transmission Control Protocol*) ofrece un servicio CONS fiable, con lo que los paquetes (aquí llamados mensajes) llegan ordenados y sin errores. TCP se ocupa también del control de flujo extremo a extremo, para evitar que por ejemplo un *host* rápido sature a un receptor mas lento. Ejemplos de protocolos de aplicación que utilizan TCP son el SMTP (*Simple Mail Transfer Program*, correo electrónico) y el FTP *(File Transfer Program*).



segmento TCP

El otro protocolo de transporte es UDP (*User Datagram Protocol*) que da un servicio CLNS, no fiable. UDP no realiza control de errores ni de flujo. Una aplicación típica donde se utiliza UDP es la transmisión de voz y vídeo en tiempo real; aquí el retardo que introduciría el control de errores produciría mas daño que beneficio: es preferible perder algún paquete que retransmitirlo fuera de tiempo. Otro ejemplo de aplicación que utiliza UDP es el NFS (*Network File System*); aquí el control de errores y de flujo se realiza en la capa de aplicación.



UDP

La capa de aplicación TCP/IP

Esta capa desarrolla las funciones de las capas de sesión, presentación y aplicación del modelo OSI. La experiencia ha demostrado que las capas de sesión y presentación son de poca utilidad, debido a su escaso contenido, por lo que la aproximación adoptada por el modelo TCP/IP parece mas acertada.

La capa de aplicación contiene todos los protocolos de alto nivel que se utilizan para ofrecer servicios a los usuarios. Entre estos podemos mencionar tanto los 'tradicionales', que existen desde que se creó el TCP/IP: terminal virtual (*TelNet*), transferencia de ficheros (FTP), correo electrónico (SMTP) y servidor de nombres (DNS), como los mas recientes, como el servicio de *news* (NNTP), el Web (HTTP), el *Gopher*, etc.

Capa	Protocolo
Aplicación	TCP/IP (DNS, SNMP, SNMP, NNTP, HTTP)

Capa	Protocolo
Transporte	TCP/IP (TCP, UDP) ATM (AAL1, AAL2, AAL3/4, AAL5)
Red	TCP/IP (IP, ICMP, ARP, RARP, OSPF, BGP, IPv6), ATM (Q2931)
Enlace	ISO(HDLC), TCP/IP (SLIP, PPP), ATM, LANs
Física	N-ISDN, B-ISDN (ATM), GSM, SONET/SDH, LANs Cable coaxial, cable UTP, fibra óptica, microondas, radio-enlaces, satélite

Como ya se ha indicado, Internet es una red a través de la cual se encuentran interconectadas una gran cantidad de redes de ordenadores, de forma que cada ordenador puede comunicarse con cualquier otro, independientemente del tipo que sea o del sistema operativo que utilice (UNIX, VMS, Windows XP, DOS, OS/2, etc). Para que ésto sea posible los ordenadores deben "hablar" el mismo lenguaje, es decir, deben utilizar el mismo **protocolo de comunicaciones**.

Es relativamente fácil comprender que un cable pueda llevar información de un lugar a otro. Sin embargo, ya se sabe que Internet puede hacer que la información llegue a distintos destinos distribuidos a lo largo de todo el mundo ¿Cómo sucede ésto?

En primer lugar, la información que se envían los ordenadores se agrupa en uno o varios **paquetes de información**. Cada uno de estos paquetes tiene su dirección de origen y dirección de destino. Por lo tanto, un conjunto de paquetes constituirá un mensaje.

Las diferentes partes o subredes que constituyen Internet se encuentran conectadas por un conjunto de computadoras especializadas denominadas **enrutadores** (*routers*), que interconectan redes. Si los ordenadores o *host*s que intercambian información se encuentran en la misma red local, es la propia red la que sirve de soporte para que dos máquinas intercambien paquetes, y si no, son los ***routers*** los encargados de decidir como dirigir los paquetes, de forma que éstos viajen a través de otras subredes hasta llegar a su destino.

Sin embargo, no todo enrutador tiene una conexión con cada uno de los otros enrutadores de la red. Una computadora manda los paquetes a la red, si su dirección es local, los paquetes llegan directamente a la máquina destino a través de la red local. Si la dirección es la de una máquina en otra subred, es entonces el *router* el encargado de tomar dichos paquetes, examinar la dirección destino y de entre sus enlaces (*router* / máquinas) decidir cuál es el más apropiado para que el paquete llegue a su destino. De esta manera actuarán sucesivamente los distintos *routers* de forma que los datos podrían atravesar varias subredes y *routers* hasta conseguir llegar al destino final.

El Programa Inetd y los Puertos

Cada vez que una máquina solicita una conexión a otra, especifica una dirección particular. En general, está dirección será la dirección IP Internet de dicha máquina. Pero hablando con más detalle, la máquina solicitante especificará también la aplicación que está intentando alcanzar dicho destino. Esto involucra a dos elementos: un programa llamado *inetd* y un sistema basado en *puertos*.

Inetd. *Inetd* pertenece a un grupo de programas llamados TSR (*Terminate and stay resident*). Dichos programas siempre están en ejecución, a la espera de que se produzca algún suceso determinado en el sistema. Cuando dicho suceso ocurre, el TSR lleva a cabo la tarea para la que está programado.

En el caso de inetd, su finalidad es estar a la espera de que se produzca alguna solicitud de conexión del exterior. Cuando esto ocurre, *inetd* evalúa dicha solicitud determinando que servicio está solicitando la máquina remota y le pasa el control a dicho servicio. Por ejemplo, si la máquina remota solicita una página web, le pasará la solicitud al proceso del servidor Web.

En general, *inetd* es iniciado al arrancar el sistema y permanece residente (a la escucha) hasta que apagamos el equipo o hasta que el operador del sistema finaliza expresamente dicho proceso.

Puertos. La mayoría de las aplicaciones TCP/IP tienen una filosofía de cliente-servidor. Cuando se recibe una solicitud de conexión, inetd inicia un programa servidor que se encargará de comunicarse con la máquina cliente. Para facilitar este proceso, a cada aplicación (FTP o *Telnet*, por ejemplo) se le asigna una única dirección. Dicha dirección se llama *puerto*. Cuando se produce una solicitud de conexión a dicho puerto, se ejecutará la aplicación correspondiente.

Aunque la asignación de puertos a los diferentes servicios es de libre elección para los administradores de sistema, existe un estándar en este sentido que es conveniente seguir. La tabla que se muestra a continuación presenta un listado de algunas asignaciones estándar:

Servicio o Aplicación	*Puerto*
File Transfer Protocol (FTP)	21
Telnet	23
Simple Mail Transfer Protocol (SMTP)	25
Gopher	70
Finger	79
Hypertext Transfer Protocol (HTTP)	80
Network News Transfer Protocol (NNTP)	119

1.4 Direcciones IP

Dirección física: Cada tarjeta controladora de red debe tener una única dirección. En una red, para que un proceso se pueda comunicar con otro, debe conocer su dirección o tener algún mecanismo para poder encontrarla.

Hay varios niveles de direcciones. Los protocolos de más bajo nivel deben usar direcciones físicas. Por ejemplo, **Ethernet** usa una *dirección física* de 48 bits fijada en el *hardware* de cada tarjeta controladora de red. La **IEEE** asigna rangos de números a los fabricantes de tarjetas controladoras de **Ethernet** para que las direcciones sean únicas.

La capa **IP** del protocolo usa el protocolo **ARP** (Protocolo de Resolución de Direcciones) para convertir las direcciones **Internet** en direcciones **Ethernet**. Existe también el protocolo RARP (*Reverse Address Resolution Protocol*), Protocolo de Resolución Inversa de Direcciones. Su función es encontrar la dirección IP a partir de la dirección física.

Las redes interconectadas a **Internet** no tienen por qué disponer de un mismo mecanismo de direccionamiento en los diferentes nodos. Por ello es necesario dar una **dirección lógica** a cada máquina.

El protocolo **IP** define una dirección de 32 bits. A cada ordenador conectado a la **red Internet** se le asigna una *dirección lógica* denominada número de *internet* o dirección **IP**.

Esta dirección está formada por 32 bits, separados en cuatro grupos de 8 bits, que se escriben como 4 números decimales con valores comprendidos entre el 0 y el 255 separados por "." . Formato D.D.D.D.

Los cuatro grupos que forman la dirección Internet se dividen en dos partes, la primera corresponde a la dirección de la red y la segunda a la dirección de máquina (*host*).

Parte	Descripción
Número de red	Debe ser el mismo para todas las máquinas conectadas a la misma red. Dos redes no pueden tener el mismo número.
Numero de máquina	Dos máquinas de la misma red no pueden tener el mismo número.

- Una parte que identifica la dirección de la red (NETID). Esta parte es asignada por el NIC (*Network Information Center*). En España se encarga de asignar estas direcciones un organismo público. Si la red local no va a conectarse con otras redes, no es necesario solicitar a ese organismo una dirección. El número de bits que ocupa esta parte depende del tamaño de la red y puede ser 8, 16 ó 24.
- Una parte que identifica la dirección de la máquina dentro de la red (*host*ID). Las direcciones de los *hosts* son asignadas por el administrador de la red.

1.4.1 Direcciones de red

Las direcciones de red son asignadas por **NIC** (***N**etwork **I**nformation **C**enter*) cuando se les solicita.

Dependiendo de sus necesidades (número de subredes, número de ordenadores...), una red puede ser de una de las clases: A, B o C. Se utilizan 8, 16, ó 24 bits para identificar la red según sean de tipo A, B o C, y el resto sirven para identificar las distintas máquinas dentro de la red.

Las clases de redes se distinguen según el valor del primer dígito de la dirección lógica de *internet*:

Valor	Clase de red	Formato
001..126:	IP clase A	--> N.H.H.H
128..191:	IP clase B	--> N.N.H.H
192..223:	IP clase C	--> N.N.N.H
224..254:	IP clase D, E, F	--> N.N.N.H

N: parte correspondiente a la red.

H: parte correspondiente al ordenador.

Las redes de clase A

Usan los primeros 8 bit para el número de red y los restantes 24 bits para el número de máquina. Son para las redes de tamaño grande. Permite un número pequeño de redes con muchas máquinas cada una. El formato de las direcciones es el de la figura:

1……..7	8……..32
Dirección de la red 0…..	Identificador de la máquina

La parte que identifica la red consta de

- un cero (0)
- 7 bits más.

El posible definir un máximo de 126 (2^7-2) redes de este tipo y cada red soporta un máximo de 16.777.214 (2^24-2) *host*s. Obsérvese que hemos restado dos números de red y dos números de *host*. Estos números no pueden ser asignados ni a ninguna red ni a ningún *host* y son usados para propósitos especiales. Por ejemplo, el número de *host* "todos 0" identifica a la propia red a la que "pertenece". El rango de direcciones para la redes de clase A es de 1.xxx.xxx.xxx hasta 126.xxx.xxx.xxx

Las redes de clase B

Usan los 16 primeros bits para el número de red y los 16 restantes para número de máquinas de cada red.

Son redes de tamaño mediano que tienen entre 2^8 y 2^{16} *host*s. La parte que identifica la red consta de

- La secuencia uno-cero (10).
- 14 bits con cualquier valor.

Esto nos da un máximo de 16.384 (2^14) redes de este tipo, pudiéndose definir en cada una de ellas hasta 65.534 (2^16-2) *host*s. El rango de direcciones para la redes clase B es de128.0.xxx.xxx hasta 191.255.xxx.xxx. El formato de las direcciones es:

1……..……16	17……..……..32
Dirección de la red 10…..	Identificador de la máquina

Las redes de clase C

Usan los 24 primeros bits para números de red y los 8 bits restantes para número de máquinas dentro de cada red.

La parte que identifica la red consta de

- La secuencia uno-uno-cero (110).
- 21 bits con cualquier valor.

Por tanto, el rango de valores para el primer byte de los dos asignados a la red es de : 192-223.

Tenemos así 2.097.152 (2^21) redes posibles con un máximo de 254 (2^8-2) *host* por red. El rango de direcciones en notación decimal para las redes clase C sería de 192.0.0.xxx hasta 223.255.255.xxx. El formato de las direcciones es:

1…….....…….……24	25……..……..32
Dirección de la red 110…..	Identificador de la máquina

1.4.2 Direcciones de máquinas

Las direcciones de las máquinas las asigna el responsable de la red. Como ya hemos visto, según el tipo de red que sea, para la dirección de la máquina quedarán, 24, 16 u 8 bits.

El número de máquinas que puede tener cada tipo de red es el siguiente:

Una red tipo A, puede tener 16.777.216 máquina. (256x256x256)

Una red tipo B, puede tener 65.534 máquinas (256x256)

Una red tipo C, puede tener 254 máquinas.

Redes de tipo A pueden haber 126. De tipo B, 16.534 y de tipo C cerca de dos millones de redes. Multiplique el número de redes posibles de cada tipo por el número de máquinas de cada tipo y sabremos el número total de máquinas que se pueden direccionar con este formato.

	Byte 1	**Byte 2**	**Byte 3**	**Byte 3**
Clase A	0…126	0…255	0…255	0…255
Clase B	128 …191	0…255	0…255	0…255
Clase C	192…223	0…255	0…255	0…255

Dirección Internet	clase	Número de red	N1 de Máquina
16.126.16.250	A	16	126.16.250
130.180.23.45	B	130.180	23.45
195.100.78.50	C	195.100.78	50

Ejemplo:

Red tipo A con subred. 06.01.128.157

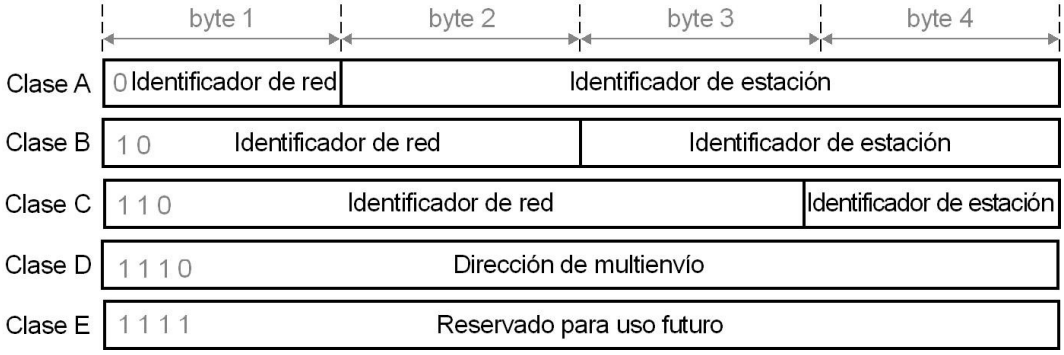
06: número de red.

01: número de subred de la red 6

128:157: número del *host* (nodo)

Tipo	X	X	X	X
Reservada	0			
Clase A	1-126	M Á Q U I N A (*host*)		
Reservada	127			
Clase B	128-191	. 1-254	M A Q U I N A *(host)*	
Clase C	192-223 .	1-254	. 1-254	MÁQUINA
Clase D	224-239	reservadas		
Clase E y F	240-255	reservadas		

Las *direcciones* entre 224.0.0.0 y 239.0.0.0 corresponden a la clase D, reservadas para transmisión de mensajes múltiples en la red. Las direcciones 240-255 corresponden a las redes de tipo E y F, y están reservadas para usos futuros y experimentales.



1.4.3 Convenciones de direcciones especiales

Existen algunas direcciones (combinaciones de unos y ceros) que no se asignan con direcciones IP, sin que tienen un significado especial.

Las direcciones de máquinas todos a cero o todos a uno no se pueden utilizar como direcciones de *host*, están reservadas para tareas de difusión. Los valores 0, 127 y 255 tienen un significado especial en una dirección IP.

- Una dirección que empiece con un cero hace referencia al nodo local dentro de su red actual. Por ejemplo, 0.0.0.23 hace referencia a la estación de trabajo 23 en la actual red. La dirección 0.0.0.0. hace referencia a la estación de trabajo actual.
- La dirección de bucle interno 127 es importante en procesos de resolución de problemas y diagnosis de la red. La dirección 127.0.0.0 es un bucle interno local dentro de una estación de trabajo.
- La dirección de todos los bits a uno (255 ó 255.255) designa al conjunto de todas las máquinas de la red. Se utiliza para mandar mensajes a todas las máquinas (*broadcast*). Por tanto, 192.18.255.255 envía un mensaje a todos los nodos de la red 192.18.

Estas combinaciones son:

dirección de la red	Todo unos

Esta dirección se llama difusión dirigida y permite direccionar a todas las máquinas dentro de la red especificada. Es un direccionamiento muy útil, ya que con un solo paquete podemos enviar el mismo mensaje a todas las máquinas de una red.

127	Cualquier combinación (normalmente 1)

Esta dirección se denomina **loopback** y se utiliza para realizar pruebas y comunicaciones entre procesos dentro de una misma máquina. Si un programa envía un mensaje a esta dirección, TCP/IP le devolverá los datos sin enviar nada a la red, aunque se comporta como si lo hubiera hecho.

Parte de la red a ceros	dirección de *host*

Esta dirección permite direccionar a un *host* interno de la red.

Todos unos	Todos unos

Esta dirección se denomina difusión limitada; realiza un direccionamiento a todos los *host* de la

propia red.

Todos ceros	Todos ceros

Esta dirección, direcciona al propio *host*.

Una dirección Internet no identifica a un *host*, sino a una conexión a red. Un ejemplo : si se dispone de un *gateway* que conecta una red con otra, ¿qué dirección de Internet se le da a esta estación?, ya que tiene dos posibles direcciones, una por cada red a la que esté conectada. En realidad, se le asigna a cada estación tantas direcciones IP como conexiones a redes tenga la estación.

1.4.4 Direcciones privadas

Id. de red privada	Máscara de subred	Intervalo de direcciones IP
10.0.0.0	255.0.0.0	10.0.0.1 - 10.255.255.254
172.16.0.0	255.240.0.0	172.16.0.1 - 172.31.255.254
192.168.0.0	255.255.0.0	192.168.0.1 - 192.168.255.254

1.4.5 Subredes

En 1985 se define el concepto de subred, o división de un número de red Clase A, B o C, en partes más pequeñas. Dicho concepto es introducido para subsanar algunos de los problemas que estaban empezando a producirse con la clasificación del direccionamiento de dos niveles jerárquicos.

- Las tablas de enrutamiento de Internet estaban empezando a crecer.
- Los administradores locales necesitaban solicitar otro número de red de Internet antes de que una nueva red se pudiese instalar en su empresa.

Ambos problemas fueron abordados añadiendo otro nivel de jerarquía, creándose una jerarquía a tres niveles en la estructura del direccionamiento IP. La idea consistió en dividir la parte dedicada al número de *host* en dos partes: el número de subred y el número de *host* en esa subred:

Jerarquía a dos Niveles

Prefijo de Red	Número de *host*
135.146	91.26

Jerarquía a tres Niveles

Prefijo de Red	Número de Subred	Número de *host*
135.146	91	26

Este sistema aborda el problema del crecimiento de las tablas de enrutamiento, asegurando que la división de una red en subredes nunca es visible fuera de la red privada de una organización. Los *routers* dentro de la organización privada necesitan diferenciar entre las subredes individuales, pero en lo que se refiere a los *routers* de Internet, todas las subredes de una organización están agrupadas en una sola entrada de la tabla de rutas. Esto permite al administrador local introducir la complejidad que desee en la red privada, sin afectar al tamaño de las tablas de rutas de Internet.

Por otra parte, sólo hará falta asignar a la organización un único número de red (de las clases A,B o C) o como mucho unos pocos. La propia organización se encargará entonces de asignar distintos números de subred para cada una de sus redes internas. Esto evita en la medida de lo posible el agotamiento de los números IP disponibles.

Máscara de Subred

Prefijo de Red extendido. Los *routers* de Internet usan solamente *el prefijo de red* de la dirección de destino para encaminar el tráfico hacia un entorno con subredes. Los *routers* dentro del entorno con subredes usan *el prefijo de red extendido* para encaminar el tráfico entre las subredes. El *prefijo de red extendido* está compuesto por el prefijo de red y el número de subred:

Prefijo de Red Extendido		
Prefijo de Red	Número de Subred	Número de *host*

El prefijo de red extendido se identifica a través de la *máscara de subred*. Por ejemplo, si consideramos la red clase B 135.146.0.0 y queremos usar el tercer octeto completo para representar el número de subred, deberemos especificar la máscara de subred 255.255.255.0

Entre los bits en la máscara de subred y la dirección de Internet existe una correspondencia uno a uno. Los bits de la máscara de subred están a 1 si el sistema que examina la dirección debe tratar los bits correspondientes en la dirección IP como parte del prefijo de red extendido. Los bits de la máscara están a 0 si el sistema debe considerar los bits como parte del número de *host*. Esto se ilustra en la siguiente figura:

		prefijo de red		nº subred	nº *host*
Dirección IP	135.146.91.26	10000111	10010010	01011011	00011010
Máscara de Subred	255.255.255.0	11111111	11111111	11111111	00000000
		prefijo de red extendido			

En lo que sigue nos referiremos a la *longitud del prefijo de red extendido* más que a la máscara de subred, aunque indican lo mismo. La longitud del prefijo es igual al número de bits a 1 contiguos en la máscara de subred. De este modo, la dirección 135.146.91.26 con una máscara de subred 255.255.255.0 podrá expresarse también de la forma 135.146.91.26/24, lo que resulta más compacto y fácil de entender.

Caso práctico

Pero veamos un caso práctico para comprender mejor esta clasificación con tres niveles jerárquicos. A una organización se le ha asignado el número de red 193.1.1.0/24 (esto es, una clase C) y dicha organización necesita definir seis subredes. La subred más grande puede contener un máximo de 25 *host*s.

Primer paso (definir la máscara de subred). Lo primero que debemos hacer es determinar el número de bits necesarios para definir las 6 subredes. Dada la naturaleza del sistema de numeración binario esto sólo puede hacerse tomando múltiplos de 2. Así que cogeremos 2^3=8 y podemos dejar las 2 subredes restantes previendo un eventual crecimiento de nuestra red.

Como 8=2^3, se necesitan 3 bits para numerar las 8 subredes. Como estamos hablando de una clase C , sumamos 3 y nuestro prefijo de red extendido será /27 que en decimal nos daría la máscara 255.255.255.224. Esto se ilustra en la figura siguiente:

	prefijo de red			bits nº subr	bits nº *host*
193.1.1.0/24=	11000001	00000001	00000001	000	00000
	prefijo de red extendido				
255.255.255.224=	11111111	11111111	11111111	111	00000
	27 bits				

NOTA: Para no desanimarse, podemos coger la calculadora y hacer la conversión de 11100000 a decimal, que dará justamente 224.

Segundo paso (definir los números de subred)**.** Las ocho subredes se numerarán de 0 a 7. Lo único que tenemos que hacer es colocar la representación binaria de dichos números en el campo *bits nº subred* de la primera fila de la figura anterior, y luego traducir las direcciones binarias a decimal. Quedaría lo siguiente:

Red Base: 11000001.00000001.00000001.00000000=193.1.1.0/24

Subred 0: 11000001.00000001.00000001.**000**00000=193.1.1.0/27
Subred 1: 11000001.00000001.00000001.**001**00000=193.1.1.32/27
Subred 2: 11000001.00000001.00000001.**010**00000=193.1.1.64/27
Subred 3: 11000001.00000001.00000001.**011**00000=193.1.1.96/27
Subred 4: 11000001.00000001.00000001.**100**00000=193.1.1.128/27
Subred 5: 11000001.00000001.00000001.**101**00000=193.1.1.160/27
Subred 6: 11000001.00000001.00000001.**110**00000=193.1.1.192/27
Subred 7: 11000001.00000001.00000001.**111**00000=193.1.1.224/27

Tercer paso (definir los números de *host*). En nuestro ejemplo, disponemos de 5 bits en el campo *bits nº host* de cada dirección de subred. Esto nos da un bloque de 30 (=2^5-2) direcciones de *host* posibles, que cubre los 25 que se preven como máximo. Obsérvese que restamos 2 pues las direcciones de *host* todos 0 (esta subred) o todos 1 (broadcast) no pueden usarse. Los *host* de cada subred se numeran del 0 al 30. Para definir la dirección asignada al *host* n de una subred dada, colocaremos la representación binaria de n en el campo *bits nº host* y luego traduciremos la dirección completa a notación decimal. Por ejemplo, para la subred 2 quedaría:

Subred 2: 11000001.00000001.00000001.010**00000**=193.1.1.64/24
host 1: 11000001.00000001.00000001.010**00001**=193.1.1.65/27
host 2: 11000001.00000001.00000001.010**00010**=193.1.1.66/27
host 3: 11000001.00000001.00000001.010**00011**=193.1.1.67/27
.
.
.
host 29: 11000001.00000001.00000001.010**11101**=193.1.1.93/27
host 30: 11000001.00000001.00000001.010**11110**=193.1.1.94/27

En el ejemplo anterior, la parte inicial de cada dirección identifica el prefijo de red extendido, mientras que los dígitos en negrita indican el campo de 5 bits número de *host*.

1.5 Sistemas de nombres por Dominios

1.5.1 La norma FQDN

Como las direcciones numéricas son difíciles de recordar, en **internet** se utiliza otro modo de nombrar las máquinas más fácil de recordar: el direccionamiento por dominios.

Como ya se ha apuntado anteriormente, todo proceso de comunicación entre dos máquinas en la red Internet conlleva un intercambio de paquetes. Cada máquina tiene una dirección única en Internet. Estas direcciones tienen el formato de cuatro números de 0 a 255 separados por puntos. Por ejemplo, una dirección de máquina en Internet podría ser 150.214.71.37. Este número es conocido como dirección Internet o número IP.

Al comienzo de Internet la gente aceptaba relativamente los combinaciones de números como dominios para que las máquinas se comunicasen entre sí. Sin embargo, las personas prefieren utilizar nombres, que son más fáciles de recordar que los números para identificar a un *host*. A cada dirección numérica le corresponde un nombre de estilo dominio (*domain-style*). La norma **FQDN** (nombre totalmente cualificado= *Full-Qualified Domain Name*) es la norma del direccionamiento por dominios

Todas las aplicaciones Internet permiten el uso de nombres en lugar de combinaciones numéricas para definir los dominios de una computadora. Sin embargo, los nombres también tienen problemas implícitos, ya que hay que asegurarse de que nunca dos ordenadores de Internet se denominen con igual nombre. Además es necesario tener una forma de convertir los nombres a las combinaciones numéricas apropiadas.

Al sistema utilizado para realizar todo este proceso se le denomina **Sistema de Nombres por Dominio** o **DNS**. El **DNS** es un método para asignar nombres a los *host* a través de una estructura jerárquica. Los nombres están formados por palabras separadas por puntos. Cada palabra representa un subdominio que a su vez está comprendido en un subdominio de mayor alcance. El nombre de dominio de un *host* tiene en general el siguiente formato:

usuario@dominioN...dominio3.dominio2.dominio1

- *usuario* es la persona.
- *Dominios*: nombres jerárquicos que van de menor a mayor cobertura, separados por puntos.

nom_ord.dom1.dom2...dominio_mayor

El Dominio de más alto nivel, (dominios de primer nivel *top-level-domain*) tiene dos estilos:

1.- **Genérico** (estilo descriptivo) usado para sitios de América del norte, consistente en tres letras con el siguiente significado.

com Organizaciones comerciales (DEC, Convex, IBM..).
gov Organismo gubernamental (NASA...).
edu Institución educacional (MIT...).
int Organización internacional.
mil Organización militar.
net Organismo de redes.
org Otras organizaciones.

El desarrollo mundial de la Red y la saturación de los dominios genéricos, sobre todo .com, han provocado una reacción internacional, que propone la creación de nuevos dominios genéricos: .aero, .biz, .coop, .info, .museum, .name y .pro. Ver en http://www.iana.org/gtld/gtld.htm

2- P**or países**, internacional, formado por dos letras que indican el país.

Dominio	País	Dominio	País	Dominio	País
ar	Argentina	fo	Islas Faroe	jp	Japón
at	Austria	fr	Francia	ki	Kiritabi
au	Australia	uk	Gran Bretaña	mx	México
be	Bélgica	bg	Bulgaria	nl	Holanda
gr	Grecia	bn	Brunei Darussalam	se	Suecia
u	Hungría	br	Brasil	de	Alemania
ie	Irlanda	ca	Canadá	dk	Dinamarca
in	India	ch	Suiza	es	España
it	Italia	cl	Chile	fi	Finlandia

El nuevo dominio geográfico, ".eu", servirá como elemento identificador de la Unión Europea y como forma de integración entre sus países miembro.

Puedes consultar en esta dirección información sobre los dominios http://www.iana.org/ y de todos los dominios en http://www.iana.org/cctld/cctld-whois.htm

1.5.2 Qué es ICANN?

Internet Corporation for Assigned Names and Numbers (ICANN) es una organización sin fines de lucro que opera a nivel internacional, responsable de asignar espacio de direcciones numéricas de protocolo de Internet (IP), identificadores de protocolo y de las funciones de gestión o administración del sistema de nombres de dominio de primer nivel genéricos (gTLD) y de códigos de países (ccTLD), así como de la administración del sistema de servidores raíz. Aunque en un principio estos servicios los desempeñaba *Internet Assigned Numbers Authority* (IANA) y otras entidades bajo contrato con el gobierno de EE.UU., actualmente son responsabilidad de ICANN.

Como asociación privada-pública, ICANN está dedicada a preservar la estabilidad operacional de Internet, promover la competencia, lograr una amplia representación de las comunidades mundiales de Internet y desarrollar las normativas adecuadas a su misión por medio de procesos "de abajo hacia arriba" basados en el consenso. Información sobre ICANN en:

- http://www.icann.org/
- http://www.icann.org/tr/spanish.html

- http://www.internic.net/

1.5.3 Registrar un dominio .es

Para realizar el registro de un dominio .es podemos acudir al Registro Delegado de Internet en España (http://www.nic.es) , o a empresas registradoras o los proveedores de servicios de Internet que pueden realizar estos trámites por nosotros.

Registradores de dominios

- http://www.arsys.es/
- http://www.acens.com/
- http://www.nominalia.es/

Para conflictos de dominios

- http://www.wipo.int/portal/index.html.es organización internacional de la propiedad intelectual
- http://www.icann.org/dndr/udrp/policy.htm

Darse de alta en google

- http://www.google.com/addurl/?hl=es&continue=/addurl

1.5.4 Hospedaje de la Página (*hosting*)

Modelos de Hospedaje

***host*ing (alojamiento compartido)**

Una empresa proveedora de servicios Internet alquila espacio de uno de sus servidores para que alojemos nuestra WEB, y que ésta sea así accesible desde Internet.

En ese servidor, residen también las páginas de otras empresas.

La empresa proveedora de servicios Internet se encargará del mantenimiento de este servidor compartido. El *hosting* es el modelo más aconsejable para la pequeñas empresas.

Servidor Dedicado

a empresa proveedora de servicios de Internet me cede (venta o alquiler) uno de sus servidores en exclusividad para nuestra empresa. Esta modalidad es más cara que la anterior.

La empresa proveedora pueden encargarse de parte del mantenimiento de ese servidor y de sus cuidados (prevención de incendios, control de intrusos, etc.). Nosotros nos tendremos que encargar de otra parte del mantenimiento (copias de seguridad, etc.). Por esto, esta modalidad requiere por nuestra parte mayores conocimientos

Housing

Alojamiento del un servidor de nuestra propiedad en las instalaciones del proveedor de servicios.

Puede ocurrir que dispongamos de un servidor Internet pero que no tengamos la infraestructura adecuada para alojarlo (línea de alta velocidad, sala con aire acondicionado, sistema de alimentación eléctrica ininterrumpida, etc.)

En esta caso, podremos “alojar” nuestro servidor en las instalaciones de un Proveedor de Servicios de Internet. Es nuestra la responsabilidad del mantenimiento de ese equipo.

Sistema operativos

Tendré que decidir que sistema operativo tendrá el servidor donde aloje mi WEB, si Linux o Windows. Los proveedores suelen dar las dos opciones.

En las dos plataformas se puede conseguir las mismas cosas para nuestra web, pero utilizaremos distintos programas para hacerlo

- Bajo un servidor Linux, utilizaremos PHP como lenguaje de programación y MySQL como sistema de gestión de base de datos. También podremos utilizar Perl o Python.
- En cambio, en un servidor Windows utilizaremos ASP y SQL Server (o Access) como base de datos, y otros productos Microsoft.

- Los servidores Linux son algo más baratos que los de Microsoft (ya que Linux y las aplicaciones para Linux son Software Libre). Los servidores Linux admiten muchas, muchas aplicaciones gratuitas (PHPNuke, OSCommerce, etc...).
- En cambio, hay muchas menos cosas "gratis" para plataformas Windows .En cambio, puede ser que los productos Microsoft sean mas fáciles de configurar o mantener que los productos Linux.

Los servicios adicionales a considerar en la contratación son los siguientes:

- **Espacio Web:** Cantidad de información que puedo alojar en el servidor. Se mide en MB o GB.
- **Cuentas de Correo**: Número de cuentas de correo asociadas a mi dominio
- **Cuenta/s FTP**: Acceso mediante un nombre de acceso y contraseña para que, a trés de FTP, podamos actualizar nuestra WEB.
- **MB de Transferencia**: No es lo mismo para el proveedor de servicio que nuestra página la vean 100 usuarios al mes que 100.000. Cada vez que un usuario consulta nuestra página, se "baja" una cierta capacidad de información, ocupando las líneas de comunicaciones del proveedor. La mayoría de las soluciones de *host*ing limitan la cantidad máxima de información que se puede bajar de mi página web (cuando se supera esta cantidad, se factura a parte). El parámetro que medirá esto serán los MB/mes o GB/mes.
- **Capacidad de programación:** Si necesito la capacidad de programar o conectar mi web con una base de datos, tendrá que asegurarme de que mi servidor me lo permita. Esto, como comentamos anteriormente, dependerá del tipo de servidor que hayamos contratado:
  - Servidor Windows: Programación ASP, Base de datos SQL Server o Access…
  - Servidor Linux: Programación PHP, Perl, Python, Base de datos MySQL
- Capacidad de crear listas de distribución, chats, etc...

FAQS

- https://www.interdominio.com/PortalServlet?pagina=/publica/faqs/faqs.jsp

Precios

- www.arsys.es/productos/tarifas/

1.5.5 Traducción de nombres

Servidores de nombres

¿Qué es el DNS?

El DNS (servicio de nombres de dominio) es el servicio responsable de realizar la conversión entre los nombres de dominio y sus correspondientes direcciones IP. Esta conversión puede realizarse en ambos sentidos: a partir de un nombre de dominio se puede obtener la dirección IP asociada y viceversa.

El DNS se utiliza para facilitar la identificación de los sistemas conectados a la red por parte de los seres humanos. A todos nosotros nos resulta mucho más fácil recordar un nombre de máquina que no su dirección IP.

La importancia del DNS viene a que, en su ausencia, no es posible realizar la conversión de direcciones.

DNS (*Domain Name System*) es una gigantesca base de datos distribuida. Se implementa a través de los servidores de nombres. Cada uno posee información completa sobre un subconjunto del espacio de nombre de dominio e información memorizada sobre otras porciones; además, dispone de información completa sobre su zona de autoridad.

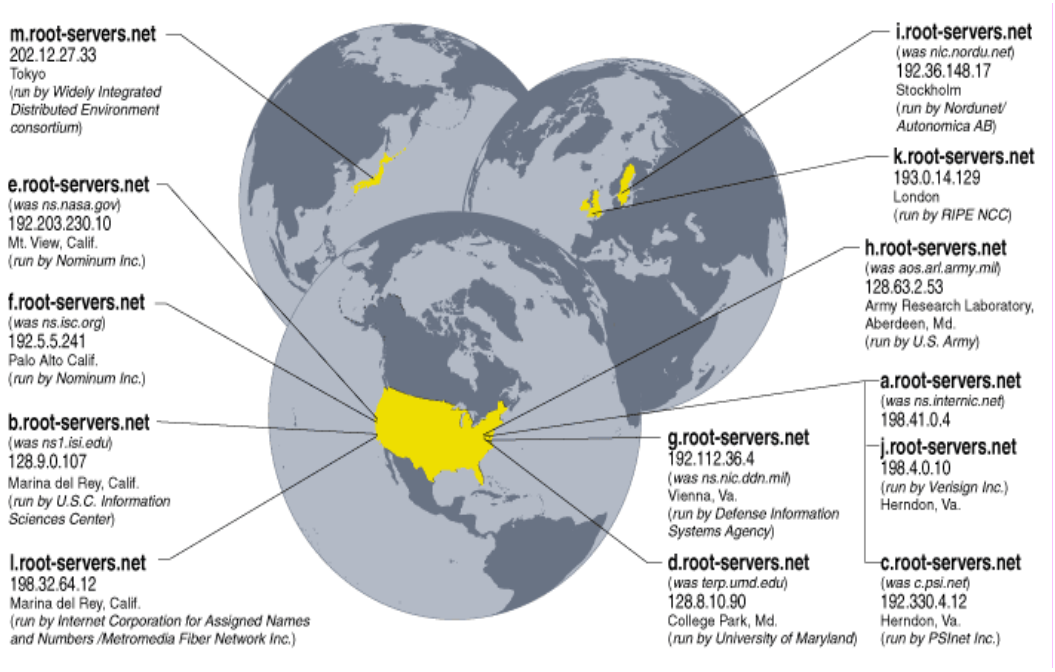
La información sobre un dominio está dividida en zonas. La información puede repartirse entre varios servidores a fin de proporcionar un servicio redundante. Cada servidor de nombre posee información sobre otros servidores de nombres responsables de diferentes zonas. Cuando llega una solicitud de información sobre la zona en la que un servidor de nombres es responsable, éste sencillamente proporciona la información. Sin embargo, cuando llega una solicitud de información de una zona diferente, el servidor de nombres se pone en contacto con el servidor de nombre correspondiente con autoridad en dicha zona.

Los servidores de nombres se clasifican en dos tipos fundamentales: primarios y secundarios. Un servidor de nombres de dominio primario es aquel que toma los datos de las zonas para las que está autorizado, desde ficheros de datos conocidos como ``db" o ficheros de base de datos (*database files)* presentes en la máquina donde se ejecuta. En cambio el secundario lo hace desde otros servidores autorizados para la zona (primarios generalmente). El proceso de actualización de la información de una zona en los servidores secundarios se conoce como transferencia de zona.

¿Qué son los servidores raíz?

Son aquellos que controlan ***el dominio raíz*** y conocen todos los servidores autorizados para los dominios de primer nivel. Estos servidores raíz disponen de punteros a todos los servidores responsables de los dominios de primer nivel: .com, .net, .org, .es, .uk, .info...

Existen 13 servidores raíz en todo el mundo: diez de ellos están situados en Estados Unidos, dos en Europa en Reino Unido y Suecia (Londres y Estocolmo) y el último en Japón. Esta distribución deja un poco que desear, ya que hay una elevada concentración de servidores en áreas geográficas muy reducidas. Así hay cuatro servidores en la costa oeste de los Estados Unidos (todos ellos en California) y seis en la costa este (cuatro en Virginia y dos en Maryland). Los interesados en conocer la ubicación de cada uno de los servidores y las organizaciones responsables de los mismos, pueden ver un mapa en http://www.quands.info/misc/websf1.gif.



¿Qué impacto tiene si los servidores raíz dejan de funcionar?

Como ya hemos indicado antes, para los usuarios el DNS es un servicio fundamental ya que, en su ausencia, nos vemos obligados a utilizar las direcciones IP para poder acceder a los sistemas existentes en la red. Cualquier intento de utilizar los nombres, si estos no están en las memorias caché de nuestro servidor de nombres, generará un error al no poder realizar la conversión.

Según diversos expertos, el servicio de resolución de nombres puede funcionar sin problemas para el usuario final siempre que exista un mínimo de cinco servidores operativos.

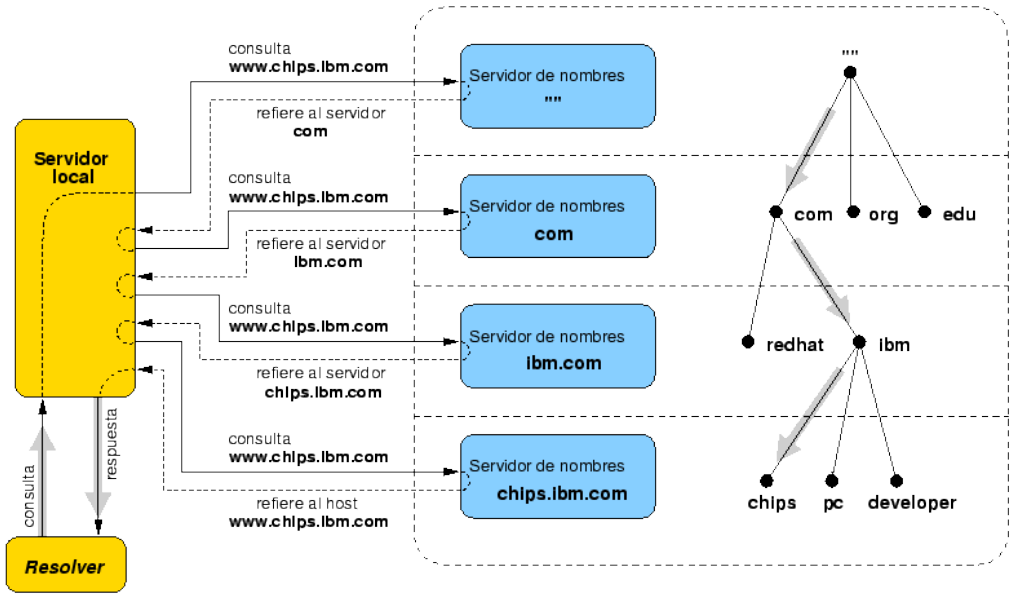
Estos servidores son claves en el proceso de resolución de nombres de dominio. Cada vez que se escribe un nombre, éste debe ser traducido a una dirección IP numérica. Cada ordenador tiene la dirección del servidor de nombres local, habitualmente configurado por el ISP. Si este servidor de nombres local no conoce la conversión a realizar, pasa la solicitud de conversión al servidor responsable del dominio (dominio de primer nivel : es com, org). En el caso de que no sepa cuál es el servidor responsable del dominio de primer nivel, realiza la consulta a uno de los servidores raíz.

Otra clase de servidor son los Servidores locales (*caching-only servers*). Los servidores locales no tienen autoridad sobre ningún dominio: se limitan a contactar con otros servidores para resolver las peticiones de los clientes DNS. Estos servidores mantienen una memoria caché con las últimas preguntas contestadas. Cada vez que un cliente DNS le formula una pregunta, primero consulta en su memoria caché. Si encuentra la dirección IP solicitada, se la devuelve al cliente; si no, consulta a otros servidores, apunta la respuesta en su memoria caché y le comunica la respuesta al cliente.

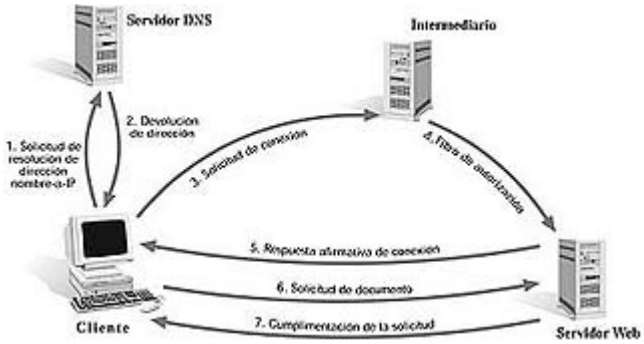
Procedimiento

Cuando un usuario introduce un URL, en su programa de navegación, el nombre debe convertirse previamente a una dirección numérica Internet, según el protocolo TCP-IP, esta misión está encomendada a unos ordenadores que funcionan como servidores de nombres (DNS).

Estos contienen unas tablas en las que a cada nombre se le asigna una dirección numérica, normalmente la petición de traducción de nombre a número llega al DNS, más cercano, que obligatoriamente tenemos que configurar en nuestro ordenador, si en este no se encuentra pasará la petición al siguiente en la jerarquía. Una vez se encuentra un servidor que puede convertir el nombre, éste nos envía de vuelta la dirección IP (número).



Por ejemplo, nuestro navegador, utilizará la dirección para confeccionar un mensaje de llamada al ordenador destino. Esta dirección será utilizada por los encaminadores o *routers* , capaces de determinar la ubicación física correspondiente a cada dirección IP, facilitando con ello la conexión entre cliente y servidor. A partir de este momento el navegador tiene un enlace con el servidor y se procesa el resto del URL, si lo hay.



La información que procede del servidor Web puede contener los siguientes parámetros:

1) Versión actual de HTTP.
2) Información del estado de la solicitud.

3) El tipo MIME, que define el formato del medio (texto, sonido, imágenes, vídeo, etc.).
4) El contenido propiamente dicho.

Una vez el servidor completa su transmisión, desactiva la conexión, ya que el usuario puede tardar algún tiempo en realizar otra petición. Si el usuario selecciona otro enlace, se negocia una conexión totalmente nueva, aunque el proceso de petición al DNS no se realice, ya que la dirección numérica se guarda en un fichero dentro del ordenador del cliente formando con ello una caché de nombres.

1.5.6 Nombres de equipos *NetBIOS* y DNS

En Windows XX pueden utilizarse dos tipos de nombres para los equipos:

- El nombre *NetBIOS*, que consta de una única parte y que será el que indiquemos en la casilla Identificación dentro del cuadro de diálogo Red en el Panel de control.
- El nombre DNS, que consta de dos partes: un nombre de *host* y un nombre de dominio, que juntos forman el nombre completo de dominio (FQDN o *Fully Qualified Domain Name)*. Este nombre se puede indicar en el cuadro de diálogo Propiedades de TCP/IP accesible también a través del cuadro de diálogo Red.

Resolución de nombres

En las redes TCP/IP, los ordenadores se identifican a través de su dirección IP. Sin embargo, a los usuarios les resulta más fácil usar nombres para los ordenadores en vez de números, por lo que se hace necesario establecer un mecanismo que resuelva nombres en direcciones IP cuando se soliciten conexiones dando los nombres de los ordenadores remotos. Esto se conoce como un sistema de resolución de nombres. En las redes existen diversos sistemas de resolución de nombres disponibles:

- **Resolución de nombres por difusión**. Cuando un equipo se conecta a la red, realizará difusiones a nivel IP para registrar su nombre *NetBIOS* anunciándolo en la red. Cada equipo en el área de difusión es responsable de cancelar cualquier intento de registrar un nombre duplicado. Uno de los problemas existentes en este sistema es que, si la red es grande, se sobrecargará de difusiones. No obstante, resultará el adecuado en una Intranet para las conexiones internas.
- **Servicio de nombres Internet de Windows (WINS, Windows Internet Naming Service)**. Utiliza una base de datos dinámica que hace corresponder nombres de equipos *NetBIOS* con direcciones IP. Dicha base de datos reside en un servidor WINS. WINS reduce el uso de la resolución por difusión y permite a los usuarios localizar fácilmente sistemas en redes remotas.
- **Resolución de nombres usando el Sistema de nombres de dominio (DNS)**. DNS permite resolver nombres DNS a direcciones IP cuando un ordenador se conecta a ordenadores remotos fuera de la red local (por ejemplo, a nodos de Internet). Necesita un servidor de nombres DNS.
- **Ficheros LM*host*S y *host*S**. Ambos ficheros se utilizan en ordenadores locales para enumerar direcciones IP conocidas de ordenadores remotos junto con sus nombres de equipo. El fichero LM*host*S especifica el nombre *NetBIOS* del ordenador remoto y su dirección IP. El fichero *host* especifica el nombre DNS y la dirección IP. Pueden considerarse como equivalentes locales a los servicios WINS y DNS y pueden usarse para resolver nombres de ordenadores remotos a direcciones IP cuando los servicios anteriores no están disponibles..

1.5.7 Relación entre direcciones IP y direcciones físicas

Se debe relacionar la dirección IP con suministrada con una dirección física. Situándose en la jerarquía de niveles utilizada por Internet, se observa que por debajo del protocolo IP existe el nivel de enlace, en el se asientan protocolos como ARP o RARP. Estos protocolos resuelven problemas relacionados con las direcciones.

- **ARP**: Convierte una dirección IP en una dirección física.

- **RARP**: Convierte una dirección física en una dirección IP.

En cada *host* debe existir una tabla de encaminamiento, que está limitada a la red que pertenece. Si la dirección IP no pertenece a la red, entonces hace dirigir los paquetes IP hacia el *gateway* o *router* que esté conectado a esa red, el cual ya poseen unas tablas que referencias las redes que conocen. El contenido de estas tablas puede variar dinámicamente.

1.5.8 Identificación de los recursos mediante el URL

Cada *host* de Internet proporciona un conjunto de servicios o recursos a los que podemos acceder a través del software cliente adecuado. Si utilizásemos un software diferente para cada servicio no sería necesario indicar el tipo de servicio en la identificación del recurso. Pero la realidad actual es que el software de navegación tiende cada vez más a incorporar acceso a servicios diferentes al HTTP (por ejemplo FTP o *Gopher*) y convertir la Web en un entramado de servicios diferentes. Ha resultado necesario por tanto crear un sistema que identifique de manera inequívoca un recurso de Internet, incluyendo el tipo de servicio, el ordenador donde se encuentra y el nombre del recurso en cuestión. Dicho sistema se llama URL (*Uniform Resource Locator*). Los URL´s son las "direcciones" de los recursos de Internet y su estructura básica es la siguiente:

- método_de_acceso://direccion_del_*host*/ruta_de_acceso
  - *método_de_acceso*. Indica el tipo de servicio o protocolo utilizado (HTTP, FTP, *Gopher*, etc.). Para acceder a páginas web o documentos de hipertexto, recordemos que es HTTP.
  - *dirección_del host*. Se refiere a la dirección IP o nombre de dominio del ordenador en el que se encuentra el recurso.
  - *ruta_de_acceso*. Es opcional y puede ser el nombre de una carpeta, una ruta de acceso hasta una carpeta determinada o el nombre de un fichero con su ruta de acceso completa.
- Otras URL mas completas
  - servicio://dirección_de_la máquina:puerto/directorio/fichero"
  - //<user>:<password>@<*host*>:<port>/<url-path>

A continuación se muestran tres ejemplos de URL´s válidos :

- http://www.altavista.com (dirección de un motor de búsqueda en Internet).
- http://www.pntic.see.mec.es/index.html (página inicial del servidor del MEC).
- ftp://ftp.mcafee.com/pub (directorio público del servidor FTP de la empresa de anti-virus Mcafee).

1.6 IP VERSION 6 La próxima generación del protocolo Internet

La nueva versión del protocolo Internet (IPv6) intenta dar respuesta a algunos problemas cruciales planteados con la versión anterior (IPv4). Entre ellos podríamos destacar la disponibilidad de direcciones IP, la gestión de las direcciones, la seguridad en las transferencias de información y la optimización de las comunicaciones multimedia.

1.6.1 Direccionamiento IPv6 de 128 bits

La longitud del direccionamiento ha sido multiplicada por 4, pasando de 32 bits a 128 bits, lo que aumenta considerablemente el número de direcciones posibles. Se prevé la creación de jerarquías de direcciones para simplificar y reducir las tablas de encaminamiento de los "*routers*" en Internet. Las direcciones IPv6 se dividen en 8 grupos de 16 bits expresados en hexadecimal y separados por ":".

Por ejemplo "A500:0000:0000:0000:83AC:000E:0000:052D".

Esta notación se puede simplificar eliminando los ceros de mayor peso en cada palabra (A500:0:0:0:83AC:E:0:52D) o sustituyendo un grupo de palabras de valor cero por ":" (A500::83AC:E:0:52D).

La estructura de la dirección de IPv6 facilita la migración a partir de las redes IPv4 actuales. Una parte del espacio de direcciones de IPv6 ha sido reservado a las direcciones IPv4. Existe una convención que permite escribir direcciones IPv4 en direcciones IPv6, utilizando las dos últimas palabras. Por ejemplo, "193.146.141.4" quedaría como "0:0:0:0:0:0:193.146.141.4" o abreviando "::193.146.141.4".

Existen tres tipos de direcciones IPv6: las que hacen referencia a un único *host* (*unicast*), las que hacen referencia a múltiples *host*s (*multicast*), y un nuevo tipo que hace referencia al *host* más próximo en términos de encaminamiento (*anycast*). Las direcciones "*broadcast*" de IPv4 que van dirigidas a toda una red son tratadas en IPv6 como "*multicast*"

1.6.2 Auto-configuración

Una de las características más notorias de IPv6 es su capacidad para configurar automáticamente un puesto con una dirección IP única o bien de forma dinámica (similar a DHCP). La configuración automática también concierne a las direcciones con el antiguo formato IPv4. Sin duda esta nueva prestación reduce drásticamente la sobrecarga administrativa y de gestión de direcciones que caracterizaba hasta el momento al protocolo IP.

1.6.3 Soporte multimedia

IPv6 proporciona un soporte mejorado de aplicaciones multimedia y de tiempo real, tales como la videoconferencia, la audio-conferencia o las aplicaciones de control, gracias a la incorporación de dos nuevas características: las prioridades y las etiquetas de flujo.

La gestión de prioridades de los paquetes se realiza en función de la naturaleza de la información que transportan. Así en el caso de una videoconferencia, el audio es considerado como más importante que el vídeo y el vídeo de baja definición tendrá prioridad sobre el vídeo de alta definición.

Las etiquetas de flujo permiten a los paquetes entre dos direcciones específicas recibir una gestión particular por parte del RSVP (*Resource Reservation Protocol* – Protocolo de Reserva de Recursos) manteniendo una secuencia lógica de paquetes para garantizar el encaminamiento perfecto.

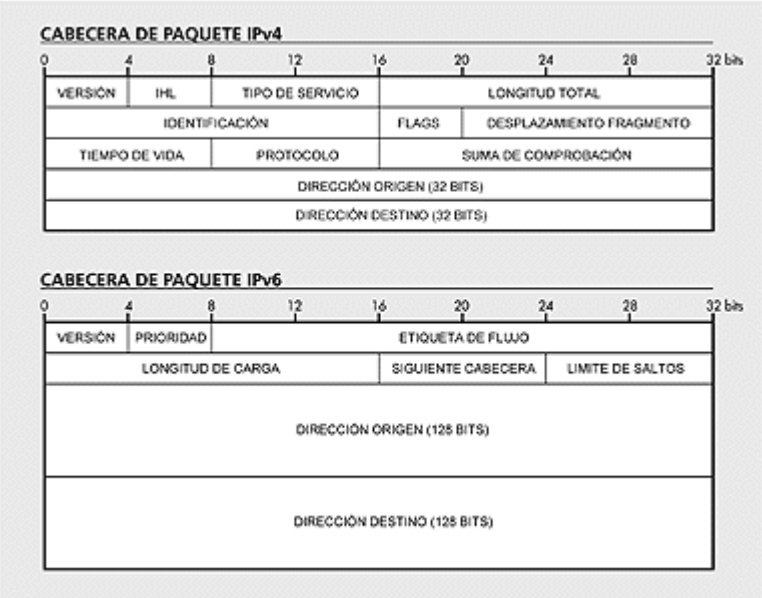
1.6.4 Seguridad

IPv6 integra la seguridad a nivel de núcleo bajo el término de IP-Sec que introduce técnicas de autenticación (permite al destinatario estar seguro del origen de un mensaje) y confidencialidad (el mensaje sólo puede ser leído por el destinatario). La autentificación está basada en MD5 y la codificación se basa en cifrado DES (*Data Encryption Standard*).

La introducción de IPv6 forzará la revisión de aplicaciones y protocolos actuales. El que parece más afectado es el servicio de nombres DNS que deberá permitir la coexistencia de las direcciones IPv4 e IPv6.

Los protocolos de encaminamiento se actualizarán para soportar IPv6, y mientras tanto deberán definirse mecanismos de "*tunneling*" que permitan transportar tráfico IPv6 sobre los *routers* actuales.

Los fabricantes de sistemas operativos y de equipos y software de comunicaciones deberán actualizar sus productos para soportar IPv6.



2 Referencias

Tutorial tcp/ip completo y avanzado

●http://ditec.um.es/laso/docs/tut-tcpip/

Conceptos de redes

- http://www.ignside.net/man/redes/index.php

DNS dinámico

- http://crysol.inf-cr.uclm.es/?q=node/25

Ver la ip

- http://www.whatismyip.com/

Los conceptos que aparecen en este tema y en otros, podéis – incluso diría que debéis – buscarlo en las enciclopedias de Internet:

- http://www.webopedia.com/
- http://en.wikipedia.org/wiki/Main_Page
- http://whatis.techtarget.com/
- http://www.pcguide.com/topic.html
- http://www.techweb.com/encyclopedia/
- http://www.techguide.com/

Direcciones con artículos

- http://www.abcdatos.com/
- http://www.monografias.com/
- http://www.conozcasuhardware.com/
- http://www.manualesgratis.com/
- http://www.auladigital.com/
- http://www.solotutoriales.com/
- http://www.tutorialesenlared.com/

Libro

- http://mhe.es/universidad/informatica/forouzan/estudiantes/estudiante_test.html
- http://highered.mcgraw-hill.com/sites/0072515848/student_view0/index.html

Bibliografía:

1. Academia de Networking de Cisco Systems. Guía del primer año. Cisco Press
2. Microsoft. Fundamentos de redes Plus. Curso oficial de certificación MCSE. McGrawHill.

3 Cuestiones

1. ¿Cuáles son los dos protocolos básicos del TCP/IP?
2. Haz un gráfico con las correspondencia entre los niveles del modelo de referencia de la ISO y los niveles de la arquitectura de internet
3. ¿Cuáles son los dos protocolos que se definen en la capa de transporte del protocolo TCP/IP?
4. Concepto de “Puerto”
5. Nombra y di las funciones principales de los dos protocolos básicos para el transporte y transmisión de datos en internet
6. Indica las clases y los formatos de las direcciones de red en internet.
7. ¿Por qué se introducen las subredes en las direcciones IP?
8. ¿Qué elementos forman el prefijo de Red extendido?
9. ¿Para que sirve la máscara de subred?
10. Explica el sistema de nombres por dominios (FQDN)
11. Funciones de un DNS
12. Indica la menos tres formas de resolución de nombres.
13. Qué diferencia hay entre los nombres de equipos en la forma *NetBIOS* y DNS?
14. ¿Cuál es la próxima versión de los protocolos para internet?
15. ¿Qué tamaño tienen las direcciones IP en la versión Ipv4? ¿Y en la versión Ipv6?
16. ¿Qué diferencia hay entre una dirección física y una lógica?
17. ¿Cuáles son las diferencias entre usar UDP y TCP?
18. ¿Cuál es la conexión que existe entre el protocolo TCP/IP y ARP?
19. Relacione el nivel de aplicación de TCP/IP con su equivalente en el modelo OSI.
20. ¿Cuáles son los protocolos físico y de enlace de datos en el conjunto de protocolos de TCP/IP?
21. ¿Cómo se denomina a los diferentes paquetes de datos en los protocolos de TCP/IP?
22. Dada una dirección IP en notación decimal-punto, ¿de qué forma se puede determinar su clase?
23. Describa la relación que existe entre la clase de la red y el número de estaciones permitido.
24. ¿Qué es un identificador de estación y un identificador de red?
25. ¿Cuál es el objetivo de emplear subredes?
26. ¿Cuál es el objetivo del protocolo ARP?
27. ¿Cuál es el objetivo del protocolo RARP?